Supervisor assessment of Master's Thesis

Student: Koscielniak Jan, Bc.
Title: Detection of Timing Side-Channels in TLS (id 23189)
Supervisor: Vojnar Tomáš, prof. Ing., Ph.D., DITS FIT BUT

1. **Assignment comments**
   Zadání práce bylo mírně obtížnější. Obtížnost spočívá zejména v tom, že se práce zaměřuje na detekci časových postranních kanálů v protokolu TLS pro zabezpečenou komunikaci na internetu. Detekce takových kanálů obecně není snadná. Zadání bylo vypsáno ve spolupráci s firmou Red Hat, kde ji vedl jako odborný vedoucí Ing. Hubert Kario. Vytvořené řešení je funkční a bylo akceptováno do hlavní vývojové větve nástroje tlsfuzzer, vyvíjeného Hubertem Kariem.
2. **Literature usage**
   Studentova práce s literaturou byla bezproblémová. Student byl schopen si nastudovat a také samostatně vyhledat potřebné materiály, a to včetně pokročilých materiálů výzkumného charakteru.
3. **Assignment activity, consultation, communication**
   Student na práci pracoval průběžně celý rok a samostatně informoval o jejích pokrocích.
4. **Assignment finalisation**
   Student práci dokončoval ve vhodném časovém horizontu, předkládal mi průběžně vytvářené verze a zapracovával mé podněty.
5. **Publications, awards**
   Práce nebyla publikována formou článku, ale její implementační část je součástí open source nástroje tlsfuzzer.
6. **Total assessment** **very good (B)**
   Práci hodnotím stupněm B s ohledem na to, že byla mírně náročnější, student na ní pracoval průběžně a aktivně a vytvořil dílo, které bylo přijato do hlavní větvě nástroje tlsfuzzer a má potenciál pro další rozvoj. Výsledky práce tak mohou být prakticky užitečné (a je zde i dosud nepotvrzená možnost, že nástroj odhalil možný časový postranní kanál v současné verzi TLS knihovny -- pokud by se tato možnost potvrdila, navrhuji komisi zvážit i případné lepší hodnocení).

In Brno 29 June 2020

Vojnar Tomáš, prof. Ing., Ph.D.
supervisor